First, some information:

In my copy of the book, there is a misprint in the statement of Fermat’s theorem (p. 56). Stated correctly, it reads: \( a^p \equiv a \pmod{p} \) for all \( a \in \mathbb{Z} \).

We can divide the problem into two cases: \( \bar{a} = \bar{0} \) and \( \bar{a} \neq \bar{0} \). In the first case, the assertion is obvious. In the second case, one sees that the non-zero elements of \( \mathbb{Z}_p \) are permuted under multiplication by \( \bar{a} \). Take it from there, or see the text. (The correct thing gets proved in the book, I’m happy to say.)

From class, 9/22. We were showing that in any group \( G \), if two elements \( a \) and \( b \) satisfied (i) \( a^6 = 1 \) and (ii) \( ab = ba^3 \), then \( a^2 = 1 \) and \( a \) and \( b \) actually commute. Since the second conclusion follows immediately from the first, we show that \( a^2 = 1 \).

Right-multiply (ii) by \( a^3 \). That gives \( aba^3 = b \). Left-multiply (ii) by \( a^{-1} \) (a.k.a. \( a^5 \)) to get \( b = a^{-1}ba^3 \). Now, cancel on the right to see \( a = a^{-1} \), and multiply by \( a \) to finish.

**Assignment 3**

Exercises 1.3: 8(a), 9(b), 12, 16, 22(b), 25(b),(d), 27(d), 34

Exercises 1.4: 2[Do (a) by direct computations of the products], 10, 12, 13(c),(d), 19[(c) and (d) only], 21, 24, 26, 29[also, relate this to the parity mapping \( \rho : S_n \rightarrow \mathbb{Z}_2 \)].

Exercises 2.1: 1(b),(h), 3(a), 9, 14, 17(a), 20

Exercises 2.2: 1(d),(f), 2, 7, 11, 20, 24, 28